

ABSTRACT

The Time to Live (TTL) field in an IP header is used as a covert channel in a communication system. More particularly the TTL field can be used to selectively mark packets with unique identifiers as they pass through an upstream station on their way to a downstream station. In this way the source of a traffic flow at least within a particular domain can be absolutely identified. This method of performing a traceback operation doesn't utilize additional resources as it relies on functionality which already exists in the system.